Certification Report

Arm Integrated Secure Element CryptoIsland-300P, version 1.0

Sponsor and developer: ***Arm Limited***
110 Fulbourn Road,
Cambridge, CB1 9NJ
UK

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-0397801-CR**
Report version:	**1**
Project number:	**0397801**
Author(s):	**Denise Cater and Jordi Mujal**
Date:	**17 August 2022**
Number of pages:	**13**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Arm Integrated Secure Element CryptoIsland-300P, version 1.0. The developer of the Arm Integrated Secure Element CryptoIsland-300P, version 1.0 is Arm Limited located in Cambridge, UK and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE (referenced as CI-300P) is a security enclave to be integrated into a SoC. The security enclave is a Hard Macro synthesized independently of other components of the SoC in combination with a Hard Macro for MRAM. It provides an isolated execution environment for executing sensitive processes and handling sensitive data, which can be used for various applications, where devices operate in a hostile environment and require a high-level of security, such as cellular subscriber identification, Smart Cards, user credentials storage, and payment. Its main usage is for Integrated SIMs.

The TOE is not itself a security enclave instantiated in hardware, but rather it is the Hard Macro of the security enclave to be integrated into an SoC.

The evaluation and certification of this TOE was performed to support reuse of the secure enclave into an SoC that is targeting conformance to *[PP0084]* as well as *[PP-0117]* to fulfil the composition requirements *[COMP]*.

In accordance with [PP0117] integration guidance is provided for the TOE. **The users of the TOE, developers of the SoC, must strictly follow the guidance and must successfully pass a (composite) evaluation of this secure enclave TOE integrated in an SoC in order for the SoC product to claim EAL4+ and/or AVA_VAN.5 resistance.** The testing was performed on a test vehicle, rather than on a sample of an instantiated TOE, as further detailed in section 2.6.3 of this report.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 17 August 2022 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Arm Integrated Secure Element CryptoIsland-300P, version 1.0, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Arm Integrated Secure Element CryptoIsland-300P, version 1.0 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures), ALC_FLR.2 (Flaw reporting procedures), ATE_DPT.2 (Testing: security enforcing modules) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Arm Integrated Secure Element CryptoIsland-300P, version 1.0 from Arm Limited located in Cambridge, UK.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	CI-300P Hard Macro[2]	Layout marking: cl145:r0p0 Digital identification: PID: D2 B0 0b 04 CID: 0D F0 05 B1
	MRAM Hard Macro[4]	MRAM_eFlash_128K x144_2019q4v1 or MRAM_eFlash_384K x144_2019q4v1
Layout Phantom View	CI-300P Hard Macro phantom view[3]	cl145:r0p0
	MRAM Hard Macro phantom view[4]	MRAM_eFlash_128K x144_PA_2019q4v1 or MRAM_eFlash_384K x144_PA_2019q4v1
Firmware & Software	FSB	1.1.1.0
	SSB	1.1.1.4
	FUT	1.3
	Runtime Library	1.1.5_1.0_1.0.6

In addition, the following manufacturing tools are delivered with the TOE:

Delivery item type	Identifier	Version
Manufacturing tools	CryptoIsland Provisioning Tools	r0p0-01eac0
	CryptoIsland HW Testing Tools	r0p0-01eac0
	CryptoIsland Disablement Tool	r0p0-00eac0
	CryptoIsland Characterization Tools	r0p0-01eac0

[2] For use by an SoC developer who has a secure development environment

[3] For use by an SoC developer who does not have a secure development environment

[4] Depending on the agreement the SoC developer has with GlobalFoundries

To ensure secure usage a set of guidance documents is provided, together with the Arm Integrated Secure Element CryptoIsland-300P, version 1.0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST-lite]*, Chapter 2.6.

2.2 Security Policy

CI-300P provides hardware-supported cryptographic services (available via a Secure cryptographic library) with fault-injection and side-channel protection:

- Random number generation
- AES key generation and destruction, as well as encryption, decryption, and authentication
- ECC key generation and destruction, as well as signature generation and verification and raw key agreement
- Hash
- Key derivation

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the *[ST-lite]*.

2.3.2 Clarification of scope

The TOE is a security enclave to be integrated into a SoC. The security enclave is a Hard Macro synthesized independently of other components of the SoC in combination with a Hard Macro for MRAM.

The evaluation and certification of this TOE was performed to support reuse of the secure enclave into an SoC that is targeting conformance to *[PP0084]* as well as *[PP-0117]* to fulfil the composition requirements *[COMP]*.

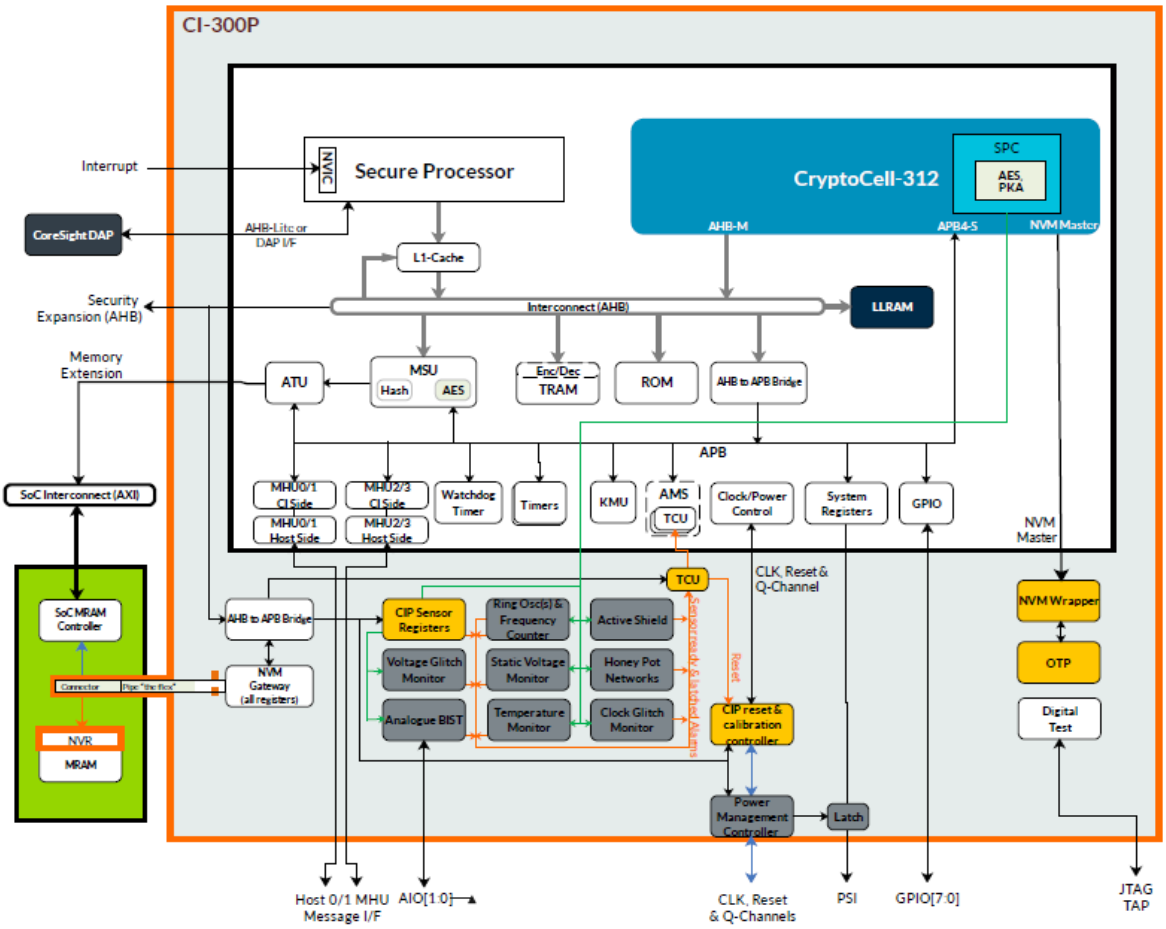
The TOE is not itself a security enclave instantiated in hardware, but rather it is the Hard Macro of the security enclave to be integrated into an SoC.

During integration of the secure enclave into an SoC, vulnerability analysis and testing of the integrated secure enclave must be performed. The *[ETRfl]* and the guidance (particularly the integration guidance *[AGD_IIG]*) will support efficient reuse.

See *[ST-lite]* chapters 4.3 and 4.4 for details regarding policies and assumptions that are to be addressed by the environment.

2.4 Architectural Information

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as below:



The TOE has the following features:

- The TOE is an isolated execution environment with its own CPU and memory subsystem. It manages its own life-cycle state that determines a security policy. Lifecycle management allows disabling test and debug features when the device is deployed.
- The TOE can run an application from Non-secure external non-volatile memory (MRAM). Running such an application is protected by MSU, which is a secured encrypted and authenticated cache.
- To protect application data residing in the external Non-secure memory against rollback, the TOE provides a non-volatile monotonic counter. The counter resides in the NVR sector of the MRAM.
- The TOE is equipped with physical protection against tampering, perturbation, and side channel leakage:
  - An active shield that protects against physical probing and provides side channel protection by generating electro-magnetic noise.
  - Environmental sensors for checking operating conditions.
  - Dedicated sensors for light detection.
  - Reset tree protection and others.
- The TOE provides parity protection for data processed by the processor, memories, and interconnects. The critical registers are protected by redundancy.
- The TOE performs memory encryption for internal RAMs (TRAM and PKA RAM) and address scrambling for TRAM.
- Cryptographic engines are protected by digital means (for example, masking), as well as with a Secure Power Convertor.
- Attacks are detected by any of these means are managed by an Alarm Management System, which routes the alarms to pre-defined safe responses aimed to prevent system operation under attacks.

- To verify that only a secure application runs on the device, the TOE provides Secure boot services achieved through a series of bootloaders (FSB, SSB). In addition, the device allows secure firmware update in the field.
- Access to various memory regions is controlled through MPU. In general, runtime firmware running on the device is considered Secure, while one internal TOE asset (device unique identity, HUK) is not accessible to the runtime firmware.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Reference	Name	Version
[AGD_PRE]	Arm® CryptoIsland™-300P Preparative Guidance	0000-04, 31 March 2022
[AGD_OPE]	Arm® CryptoIsland™-300P Operational Guidance	0000-06, 20 June 2022
[SDM]	Arm® CryptoIsland™-300P Software Developers Manual	0000-03
[AGD_SRN]	Arm® CryptoIsland™- 300P Software Release Note	4.0
[AGD_TRM]	Arm® CryptoIsland™- 300P Technical Reference Manual	0000-06, 15 April 2021
[AGD_IIG]	Arm® CryptoIsland™- 300P Hard Macro Implementation and Integration Guide	0001-06, 17 September 2021
[AGD_PTG]	Arm® CryptoIsland™- 300P Hard Macro Production Test Guide	0001-05, 17 September 2021
[AGD_MPR]	Arm® CryptoIsland™- 300P Hard Macro Qualification and Performance Report	02, 30 September 2021
[AGD_MAN]	Arm® CryptoIsland™- 300P Manufacturing Guide	0000-02, 31 March 2022
[AGD_HRN]	Arm® CryptoIsland™- 300P Hard Macro Release Note	1.0
[AGD_PEN]	Arm® CryptoIsland™- 300P Hard Macro Product Errata Notice	Version 1.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

Developer testing in development phase comprises unit and integration testing on design simulations, but also tests on physical components alone and integrated into the full chip. Software is tested also at several layers, including a full test run at the target hardware. Test environment includes Mentor Graphics Tessent and Cadence Virtuoso / Spectre Simulator tools as well as Arm dedicated test boards.

Validation testing on the final designed product is done at several layers, ranging from hardware, via all software layers, towards testing of the final TOE. Testing of software layers is automated using Jenkins.

During production, testing of the TOE integrated as part of an SOC is performed and parts of the test results are written into memory of the TOE, along with specific calibration values needed for optimal operation.

The evaluators witnessed a subset of the developer tests. The subset of tests was selected to cover various test suites, various functional aspects of the TOE, as well as areas where the code coverage approach has limitations (e.g. crypto operations). TOE identification is part of the witnessing session, as well as the methods in which code coverage has been calculated, both for software and hardware building blocks of the TOE.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV, ALC, ATE and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack-oriented analysis the protection of the TOE is analysed using the knowledge gained from all evaluation classes. This results in the identification of (additional) potential vulnerabilities. This analysis will be using the attack methods in *[JIL-AP]* and *[JIL-3S-SoC]*.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 28 weeks. During that test campaign, 27% of the total time was spent on Perturbation attacks, 64% on side-channel testing, and 9% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was performed on a test vehicle that was consistent with the TOE components described in the *[ST]*.

The TOE was tested in the following configurations:

- Hardware: CI-300P Hard Macro version cI145:r0p0
- Firmware: FSB v1.1.1.0, SSB v1.1.1.4, FUT v1.3
- Software: Runtime Library v1.1.5_1.0_1.0.6
- Test vehicle: Svalinn A1 SoC
- Test OS: Exerciser v5.9 or v5.9.2

This test configuration does not contain the MRAM that is present in the TOE. The tests were carried out on the mentioned test vehicle, which contains SRAM. The analysis of the results has taken into consideration that in the test vehicle MRAM is represented by SRAM.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

For (composite) evaluations of the TOE integrated in an SoC, please consult the *[ETRfI]* for details.

2.7 Reused Evaluation Results

There has been reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of three site certificate and Site Technical Audit Reports. Two of these site relate to the manufacturing phase 3 as defined in [PP 0117]. The third is of a data center supporting the hardware development.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Arm Integrated Secure Element CryptoIsland-300P, version 1.0. The details of the Hard Marco (GDS files) and software/firmware versions are provided in *[ST-lite]* chapter 2.5.1, Table 2-1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support evaluations of the TOE integrated in an SoC according to *[PP-0117]*, based on *[COMP]*, a derived document *[ETRfI]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is integrated in an evaluation of an SoC.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the Arm Integrated Secure Element CryptoIsland-300P, version 1.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2, ALC_FLR.2, ATE_DPT.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims ’strict’ conformance to the Protection Profile *[PP-0117]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None

3 Security Target

The Arm® CryptoIsland™-300P Integrated Secure Element Security Target, Document ID 102871, Issue 6.0, July 2022 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
ETRfI	Evaluation Technical Report for Integration
FSB	First Stage Bootloader
FUT	Firmware Update Tool
HUK	Hardware Unique Key
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LCS	Life Cycle States
MPU	Memory Protection Unit
MRAM	Magnetoresistive Random-Access Memory
MSU	Memory Secure Unit
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NVR	Non-Volatile Registers
PKA	Public Key Accelerator
PP	Protection Profile
RAM	Random-Access Memory
RTL	Resistor-Transistor Logic
3S	Secure Sub-System
SoC	System-on-Chip
SPC	Secure Power Converter
SSB	Second Stage Bootloader
TOE	Target of Evaluation
TRAM	Trusted Random-Access Memory

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report Arm Integrated Secure Element CryptoIsland-300P v1.0 – EAL4+, 21-RPT-756, v5.0, 11 August 2022
[ETRfI]	Evaluation Technical Report for Integration of Arm Integrated Secure Element CryptoIsland-300P v1.0 – EAL4+ DRAFT, 22-RPT-608, v4.0, 11 August 2022
[JIL-3S-SoC]	Guidance for Vulnerability Analysis and Penetration Testing of a Secure Sub-System within a System-on-Chip, Version 2.0 Release 4, June 2021
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[JIL-SRFPDCL]	Security requirements for post-delivery code loading, Joint Interpretation Library, Version 1.0, February 2016
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP-0084]	Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13 January 2014, registered under the reference BSI-CC-PP-0084-2014
[PP-0117]	Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, Version 1.5, 28 Feb 2022, registered under the reference BSI-CC-PP-0117-2022
[ST]	Arm® CryptoIsland™-300P Integrated Secure Element Security Target, Document ID 102871, Issue 6.0, July 2022
[ST-lite]	Arm® CryptoIsland™-300P Integrated Secure Element Security Target Lite, Document ID 107611, Issue 2.0, July 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)